ABSTRACT OF THE DISCLOSURE

In accordance with an aspect of providing trust and authentication for network communications and transactions, a network infrastructure is provided that employs biometric private keys (BioPKI). Generally, Bio PKI is a unique combination of two software solutions that validate electronic user authentication: a state-of-the-art biometric signature system, and a digital signature for data integrity. The combined solution allows networked businesses and merchants such as financial institutions to ensure that user authentication is conducted in a trusted, secure fashion within standard network environments. In one example implementation, a biometric signature augments standard digital signatures by adding an automated, non-reputable user authentication capability to the existing digital signature process. In contrast to simple verification in a pure biometric-based system or digital signature/certificate environment, BioPKI uses a combination of biometric technology to access private keys in order to create digital signatures based on biometric authentication and industry-standard PKI technologies. In one example, BioPKI utilizes public key cryptography technology to encrypt the biometric signature information for transmission to the BioPKI server. The encryption packet contains several layers of internal information to ensure that the biometric signature is secured and validated prior to accessing the individual's private key.